POSITIF: a policy-based security management system

Cataldo Basile, Antonio Lioy (Politecnico di Torino)
Gregorio Martinez Perez, Felix J. Garcia Clemente, Antonio F. Gomez Skarmeta (Universidad de Murcia)

The POSITIF project [1] – funded by the EU in FP6 – has developed a framework and tools to configure in a policy-based way the security services of networked systems and applications. This framework has been designed with the following set of interesting features in mind.

Use of a standard information model. The use of information models eases the task of building efficient and well-integrated security management systems. The POSITIF representation is based on the CIM DMTF standard [2].

Separation of system description and policy description. POSITIF separates the formal definition of the desired level of security and the target information system. In this sense, two different languages have been defined, namely P-SDL (System Description Language) and P-SPL (Security Policy Language). P-SDL describes networked systems and applications conveying the system topology, the functionality of each element, and the security capabilities of each component of the system, while P-SPL offers to security policy administrators the possibility to specify both high-level and low-level policies (i.e. it is a multi-level language).

Integration of different solutions. The integration of different solutions for the various fields of a policy-based systems is a very important goal. POSITIF has a structure permitting the coexistence of the diversity by means of a “homogenization processes”. POSITIF also supports the “biological diversity”, via the same function being implemented by different tools, to protect against failures due to bugs or errors.

Automatic derivation of rules. POSITIF deals with policy refinement: rule derivation is automatically accomplished in order to reduce the effort by the administrators. This scenario also guarantees that there are no inconsistencies between the high-level policies and the low-level rules.

Integration with IDS and IPS. A better cooperation and integration between policy specification and anomaly detection systems (such as IDS) is also supported by POSITIF. By definition, the policy is “a definite goal” and implicitly defines the desired behaviour of the information system. This information is used to detect attacks for which there is no “attack signature”, hence reducing false positives.

Openness and visibility. The POSITIF framework and related tools are open and built on official or de facto standards. In this way the solution has a wider visibility.

The framework is easy to use: the user only needs to provide a formal description of both the target networked information system and the security policy that must be satisfied. These data are processed by the Security Checker, a tool that verifies if the policy is coherent, if the security requirements can be satisfied by the given architecture and provides a rough measure of the resulting security level. Next, abstract configurations are generated to implement the security policy. They are abstract as they are block-independent and expressed in a generic format. Abstract configurations are later translated to real element-specific commands by the security technology mapper. Finally POSITIF offers the option to automatically deploy the configuration (e.g. via SNMP, SSH or proprietary solutions). Last but not least, a special security monitor tool has been developed: it goes beyond standard IDS functionality as it can generate security alarms when an event that violates the policy is detected.

Due to its modular architecture, POSITIF is very extensible. For example, new techniques and new tools can be included to improve the effectiveness of policy translation and policy checking analysis as soon as they are available.

References